JAMES M. WAGSTAFFE (95535)
MICHAEL VON LOEWENFELDT (178665)
MICHAEL NG (237915)
KERR & WAGSTAFFE LLP
101 Mission Street, 18th Floor
San Francisco, CA 94105
Tel.: 415-371-8500
Fax: 415-371-0500
Email: wagstaffe@kerrwagstaffe.com
Email: mvl@kerrwagstaffe.com
Email: mng@kerrwagstaffe.com

DAVID M. GIVEN (142375)
NICHOLAS A. CARLIN (112532)
PHILLIPS, ERLEWINE & GIVEN LLP
50 California Street, 32nd Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911
Email: dmg@phillaw.com
Email: nac@phillaw.com

Interim Co-Lead Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MARC OPPERMAN, et al.,

Plaintiffs

v.

PATH, INC., et al.,

Defendants.

Case No. 13-cv-00453-JST

CLASS ACTION

OPPERMAN PLAINTIFFS' OPPOSITION TO APP DEFENDANTS' MOTION TO DISMISS SECOND CONSOLIDATED AMENDED COMPLAINT

Hernandez v. Path, Inc., No. 12-cv-1515-JST
Pirozzi v. Apple, Inc., No. 12-cv-1529-JST
(collectively, the "Related Actions")

Date: December 2, 2014
Time: 2:00 p.m.
Courtroom: 9, 19th Floor

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Pages

Cases

Statutes

Other Authorities

I. INTRODUCTION

The facts of this case are straightforward. The "App Defendants" (all Defendants except Apple) employed Apps, made and sold by them and Apple, to harvest address book data from users' Apple iDevices, without those users' knowledge or consent, and for the App Defendants' use and benefit. Apple aided and abetted the App Defendants in this misconduct. Taken as a whole, that conduct invaded Plaintiffs' privacy and amounted to a conversion of Plaintiffs' property.

Although the Court has determined that the privacy (intrusion upon seclusion) claim was adequately pled, the App Defendants urge the Court to reach a different result through two baseless rhetorical devices. First, the App Defendants insist that, in simplifying the allegations in the latest complaint, Plaintiffs have abandoned their allegations that these Defendants misused the address book information. Plaintiffs did no such thing. They continue to allege that each App Defendant used the misappropriated address book data to benefit themselves; how precisely they did so remains a matter for discovery.

Second, the App Defendants repeat the factual argument that Plaintiffs voluntarily consented to these App Defendants' actions even, argues one App Defendant, if Plaintiffs did not know to what they were consenting. These arguments implicitly acknowledge the collective failure of the App Defendants to disclose to users what their Apps were doing. Without transparent disclosure, there cannot be knowing consent.

Leveraging these two arguments, the App Defendants restate their prior attack on Plaintiffs' privacy claim. The App Defendants' arguments that (1) they had permission, (2) their conduct was an accepted business practice, (3) there is no "reasonable expectation" of privacy in one's address book data, and (4) Plaintiffs were not injured, do not constitute a basis for departing from the Court's prior order finding this claim legally sound and properly pled.

As for the conversion claim, the App Defendants (and Apple) insist that address books and their data cannot be converted because obtaining or copying the data without permission does not deprive the owner of the ability to use it. This argument misstates California law.

California courts have repeatedly held that wrongful copying of intangible or infinitely reproducible property is conversion.

Finally, some of the App Defendants posit that Plaintiffs' claims are preempted by the Copyright Act even though all agree, incongruously, that the address books are not copyrightable subject matter in the first instance. None of their cited authorities—which all concern copyright preemption for claims based on the theft of ideas—supports a preemption defense in this case.

II. SCOPE OF OPPOSITION

This time around, the App Defendants have filed separate briefs, all making essentially the same arguments and all largely citing the same cases and each other.[1] Instagram and Kik even filed virtually identical separate motions (ECF Nos. 499, 500) through the same counsel. Apple's brief also raises the same substantive objections as the App Defendants' to Plaintiffs' conversion claim. For everyone's convenience, Plaintiffs respond to all of the App Defendants' motions and Apple's arguments on Plaintiffs' conversion claim with this consolidated opposition brief.[2]

III. ARGUMENT

A. DEFENDANTS' "NO MISUSE" AND "CONSENT" ARGUMENTS ARE BASELESS

The App Defendants tie their current round of motions to two repeated but incorrect assertions. First, they insist that Plaintiffs have "dropped," "withdrawn," or "abandoned" the allegations that their address book data was misused (as if transmitting it from the iDevice was not a misuse itself). Second, though the Court held that offering to "find friends" (or any of the other cryptic text that each used) does not generate consent to uploading or taking Plaintiffs' address books (particularly because none of the disclosures clearly asked for permission in plain

---

[1] Path only moved to dismiss Plaintiffs' conversion claim. (ECF No. 503 at 3.) As such, Path admits that Plaintiffs' invasion of privacy claim is well pled and cannot be dismissed. Similarly, Apple does not argue that Plaintiffs' invasion of privacy claim is not properly pleaded (although it does challenge the aiding and abetting allegations). (ECF No. 501.)

[2] Default has already been entered against one App Defendant, Hipster, Inc. (ECF No. 478 (hereinafter "SCAC") ¶¶ 26, 98; ECF Nos. 344, 346.) Defendants' present set of dismissal motions do not mention Hipster, and thus do not impact the Hipster Plaintiff and the prospective Hipster (sub)class' right to prosecute the SCAC/CAC's claims against Hipster and Apple.

language even though they could have done so), the App Defendants repeat the precise argument they previously lost.

1. The SCAC Continues To Allege That The App Defendants Misused Plaintiffs' Address Book Data

Though Plaintiffs shortened the SCAC by trimming excess evidentiary detail, the SCAC does not "drop" or "abandon" any material allegations.[3]

Plaintiffs still allege that the App Defendants (1) copied and obtained Plaintiffs' iDevice address books without permission,[4] (2) "misappropriated address book data as stored on the iDevices' Contacts App without authorization to do so" by "upload[ing]" the data to the App Defendant or an agent,[5] (3) "acquired a road map to users' personal lives, and were able to exploit that wrongfully obtained valuable data to grow their businesses,"[6] and (4) "benefitted substantially from its misappropriation of users' address books. On information and belief, the misappropriation of that property enabled the company to more rapidly grow its user base, avoid the costs of customer acquisition, enhance its social networking features, and increase the value of the company, among other benefits."[7]

Rule 8 does not require Plaintiffs' SCAC to describe in detail what else each individual App Defendant did with Plaintiffs' address book data after it was misappropriated. Indeed, the App Defendants have not made their specific internal practices public, so only after discovery will Plaintiffs know the true and full scope of what each App Defendant did with their

---

[3] Plaintiffs have no objection to the App Defendants insistence that the Court also consider the more lengthy allegations of the prior Complaint, but it should do so under the proper standard, i.e., while assuming the truth of those allegations. Wolfe v. Strankman, 392 F.3d 358, 362 (9th Cir. 2004).

[4] (SCAC ¶¶ 79, 141, 147, 153, 160, 167, 173, 179, 185, 191, 196, 202, 209, 215, 222, 229.)

[5] (SCAC ¶¶ 90, 94, 100, 105, 111, 115, 119, 123, 127, 131, 135.)

[6] (SCAC ¶ 60.)

[7] (SCAC ¶¶ 97, 103, 109, 113, 117, 121, 125, 129, 133, 137.)

misappropriated address book data.[8]

Regardless, neither the invasion of privacy nor the conversion claim depends on the specific use each App Defendant made of the data it misappropriated. Liability exists irrespective of any use, only the invasion itself must be highly offensive. Instead, the extent of the misuse goes to the assessment of damages. (ECF No. 471 (hereinafter "Order") at 45, n. 23.) Here, the Court already held that Plaintiffs properly pled their intrusion claim. (Id. at 46.) It should pay no regard to the notion that, after years of litigation, Plaintiffs have suddenly conceded that the App Defendants did not misuse their data. Plaintiffs allege precisely the opposite.

2. Defendants' Consent Arguments Remain Meritless

The Court already held that Plaintiffs adequately alleged there was no consent to take their address books, and that any such purported consent from a disclosure reading "scan," "find friends", or the like is invalid to confer consent. (Order at 43-45.) Nevertheless, almost all of the App Defendants continue to insist that the allegations show consent to their misconduct as a matter of law.[9] The App Defendants are still wrong and they make no real attempt to grapple with this Court's prior reasoning or to offer anything meaningful or new on the subject.[10]

Although the "presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the [plaintiff]," Hill v. Nat'l

---

[8] Path's public apology, Twitter's public admission that it kept and used the materials for 18 or more months, and copies of various other Defendants' statements and admissions and apologies have been in the Court's record for years. (E.g., ECF No. 1 at 57, 84, 89, 94; ECF No. 3 (hereinafter "FAC") at 161-63, 251-52; see also http://articles.latimes.com/2012/feb/14/business/la-fi-tn-twitter-contacts-20120214; http://blog.path.com/post/17274932484/we-are-sorry ("We are sorry. We made a mistake.").) Defendants conveniently pretend that these materials do not exist.

[9] Foursquare Labs does not make this argument, stating that it "does not adopt the arguments by Yelp and Foodspotting to the extent they rely on Plaintiffs' consent to Defendants' accessing the address books." (ECF No. 496 at 3.) As noted above, Path also does not challenge the privacy claim at all in its motion to dismiss. (ECF No. 503.)

[10] Twitter, in particular, simply restates its prior arguments that its Terms of Service or Privacy Policies demonstrate consent as a matter of law. The Court has found that they do not. (Order at 44.)

Collegiate Athletic Assn., 7 Cal. 4th 1, 37 (1994), here there was no clear and comprehensible request for permission that could support a finding of consent. Perkins v. LinkedIn Corp., No. 13-cv-04303-LHK, 2014 WL 2751053, *16-17 (N.D. Cal. June 12, 2014), on which the App Defendants rely heavily, is thus inapposite. In Perkins, the website at issue had a multi-tiered process for consent that *expressly* disclosed the actions being consented to *at each step* of the process. Id. at *1-4. The vague or non-existent disclosures here bear no relationship to those at issue in Perkins. Instead, against common rules of construction, Defendants ask the Court to read-in language that is not there.[11]

The App Defendants also argue that the allegations the Court already found sufficient to state a claim are somehow "implausible," citing In re Google Inc. Privacy Policy Litig., No. 5:12-cv-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013)[12] and In re Yahoo Mail Litig., No. 5:13-cv-04980, 2014 WL 3962824 (N.D. Cal. Aug. 12, 2014). Neither case makes it legally implausible that the App Defendants took Plaintiffs' address books without permission.

In In re Google Inc. Privacy Policy Litig., the plaintiffs' allegation that they did not realize Google would aggregate their data was in contrast to a disclosure that "if you're signed in, we may combine information that you've provided from one service with information from other services." 2013 WL 6248499 at *2, *16. In In re Yahoo Mail Litig., the court found that

---

[11] The CAC included the in-app text from each App's "disclosure" (ECF No. 362 at 63-99), which the Court already ruled amounted to no consent. (Order at 43-45.) Screenshots from most all of the Apps in suit are already contained in the FAC and elsewhere in the record. (ECF No. 3 (FAC) at 174-279.) As described in a more streamlined fashion in the SCAC, the Defendants' in-app "disclosures" were as follows: SCAC ¶ 96 (Gowalla had a "Find Friends" click through screen), ¶ 102 (Kik Interactive did not have a specific screen for consent), ¶ 108 (Path had a "Sign Up" click through screen), ¶ 112 (Foursquare Labs had a similar login/sign up click through screen), ¶ 120 (Yelp had a Find Friends button with displayed text), ¶ 124 (Twitter had a "follow your friends" click through screen), ¶ 128 (Foodspotting had a "Follow People" click through screen), ¶ 132, and ¶ 136. Plaintiffs allege that the App Defendants acted without authorization (SCAC ¶ 90), and without Plaintiffs' consent "to the taking of their data." (SCAC ¶¶ 92, 94, 100, 105, 111, 115, 119, 123, 127, 131, 135.)

[12] There are two opinions in In re Google Inc. Privacy Policy Litig. cited by defendants: No. 5:12-cv-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013) and No. 5:12-cv-01382-PSG, 2014 WL 3707508 (N.D. Cal. July 21, 2014). The facts supporting the court's decision are the same in both. As such, each is similarly distinguishable from Plaintiffs' case here.

consent to Yahoo reading and analyzing one's email as it passes through Yahoo's servers necessarily includes consent to copying the same email under the terms of the Wiretap Act. 2014 WL 3962824, at *6-9. The court applied a different analysis to the plaintiffs' privacy claim, reasoning that "a plaintiff's lack of consent does not matter so much as the nature of the information[.]" Id. at *17.

Nothing in these cases suggests that it is "implausible" that Plaintiffs did not consent to the uploading and taking of their address books. There is nothing implausible about an ordinary person's unwillingness to have their address books taken and used by the App Defendants or expectation that their privacy would be respected. Indeed, privacy surveys demonstrate that the implausible position is the App Defendants' because the vast majority of people are *not* willing to share their mobile address book's data with a social networking app. (SCAC ¶ 57.)

Defendants Yelp and Foodspotting go so far as to argue that Plaintiffs should be deemed to have consented even if they did not actually understand what they were consenting to allow. They cite no law for this radical and arrogant argument. Uninformed consent is an oxymoron.

Other App Defendants argue that they did not exceed consent because there are no allegations that they promised not to invade Plaintiffs' privacy. That turns the concept of consent on its head. No law supports the assertion that a consumer broadly consents to anything, including bad acts, that are not affirmatively disclosed.

As this Court has already determined, Plaintiffs have alleged that their address books were taken without valid, informed consent. It determined as much, at least in part, because the App Defendants' disclosures were lacking. (Order at 43-45.) The App Defendants provide no basis for the Court to revisit or change its analysis in that regard.

B. INVASION OF PRIVACY FOR INTRUSION UPON SECLUSION IS PROPERLY PLED

1. The App Defendants' Conduct Was Highly Offensive

The App Defendants try four different arguments to convince the Court their conduct was inoffensive *as a matter of law*. This is despite the Court's ruling that it is a jury question (Order at 46), the Congressional inquiry letters that many of them received, the media firestorm that engulfed the subject and these Defendants for quite some time, the public apologies that several

of them issued, and an FTC investigation and consent judgment, among other things. (SCAC ¶¶ 77-84, 101, 107.)

First, the App Defendants argue that in some cases whether an invasion is offensive can be determined as a matter of law. Where the facts are undisputed the initial threshold question may be decided as a matter of law. See Miller v. Nat'l Broad. Co., 187 Cal. App. 3d 1463, 1483 (1986) (explaining on a summary judgment motion that the court can determine whether threshold of "offensiveness" has been met, but noting that inquiry as to whether invasion of privacy was "highly offensive to a reasonable person" is a question for the jury). That does not mean, however, that the Court was wrong when it determined that in this case such threshold was met and that this now is a question "best left for a jury."[13] (Order at 46.)

Second, the App Defendants argue that they did not use Plaintiffs' iDevice address book data in a highly offensive way—an utterly unverifiable (without discovery) self-serving factual statement since they still won't reveal precisely what they took or what happened to the data once they took it. But Plaintiffs do allege the App Defendants' misuse of the data.[14] Regardless, the Court has already confirmed that allegations of use, whether offensive or not, are not necessary to sustain this claim.[15] (Order at 45, n. 23.) Moreover, were the App Defendants'

---

[13] Numerous allegations demonstrate that the App Defendants' conduct is highly offensive. (SCAC ¶¶ 56-57 (the iDevice address book is regarded as personal and private by the United States Supreme Court and consumers); ¶¶ 76-78 (Apple's representations (albeit false) that it protects users from this intrusion demonstrates that the intrusion is offensive); ¶¶ 83-84, 87 (Apple pulling of apps publically revealed to be uploading data demonstrates that it is offensive); and ¶¶ 80-81, 84 (Congress and the media's outcry after the scandal of multiple iDevice Apps copying and uploading users' iDevice address books without warning was initially exposed demonstrates offensiveness).)

[14] (SCAC ¶¶ 90-92, 94, 97, 100, 103, 105, 109, 111,113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 247, 253.)

[15] Order at 46, n. 23: "Moreover, unlike the Folgelstrom court, this Court *has* been able to locate cases which impose liability without an allegation of highly offensive use. For example, in Sanchez-Scott v. Alza Pharm., 86 Cal. App. 4th 365, 377–78 (2001), a patient adequately stated an intrusion upon seclusion claim where her doctor performed a breast examination in front of a pharmaceutical salesperson without revealing that the salesperson was not a medical professional. In that case, no "highly offensive use" was at issue, only the highly offensive manner in which the privacy interest was invaded. ¶ The Restatement also expressly disavows any such limitation. See Rest. (2d) of Torts § 652B, Comment b ("The intrusion itself makes the defendant subject to liability, even though there is no publication *or other use of any kind* of the photograph or information outlined.") (emphasis added)."

meritless theory valid, precisely what each App Defendant did with the data would require discovery, and a Rule 12(b)(6) motion would be an improper procedural vehicle for litigating this factual issue.

Third, the App Defendants argue that their conduct is not highly offensive because stealing users' iDevice address book data is a commonplace business practice that does not rise to the level of an egregious breach of social norms. As this Court has already found, the dicta the Defendants rely on in Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 993 (2011) is unpersuasive. (Order at 45-46, n. 23.) Moreover, a company itself compiling a list of information on individual customers is wholly different than taking those customers' private address books.[16]

The App Defendants' related, but equally spurious, argument that stealing Plaintiffs' iDevice contacts is not highly offensive because it is "necessary" to provide a service is simply false and, nevertheless, the type of factual argument inappropriate on a motion to dismiss. Other Apps employ transparent notification techniques and hashing to accomplish the same function—and their developers have criticized the App Defendants here for not doing the same—and thereby avoid uploading the address books or any other raw data. (FAC ¶¶ 146-149, 151, 160, 266-267, 340 at n. 193, 416-417, 501.) Moreover, Defendant's claim of "necessity" is not an exception to the requirement of disclosure and consent. (SCAC ¶ 76 (xvii), (xxi), (xxii), (xxiii), (xxviii).) Defendants' self-serving justification for their misconduct is, at best, for the jury.[17]

---

[16] As such, App Defendants' citation of other district court cases that rely on the dicta in Folgelstrom is equally misplaced. See, e.g., In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012); In re Google Android Consumer Privacy Litig., No. 11–md–02264 JSW, 2013 WL 1283236, *10 (N.D. Cal. Mar. 26, 2013). App Defendants also cite to Yunker v. Pandora Media, Inc., No. 11-cv-03113 JSW, 2013 WL 1282980, *14 (N.D. Cal. Mar. 26, 2013). That case is further distinguishable because the court found that plaintiffs voluntarily consented to providing raw personal data. Id. at *15. Here, unlike the plaintiffs in Yunker, Plaintiffs were never asked to consent to the App Defendants taking this data.

[17] Defendants' cited cases do not help their cause. Cramer v. Consolidated Freightways, Inc. addressed whether union employees' claim for invasion of privacy was preempted by their collective bargaining agreement, which has no bearing here. 209 F.3d 1122, 1128-33 (9th Cir. 2000). Likewise, a challenge to supposed after-hours video monitoring of a work space was rejected because the plaintiffs *were never actually video-taped and weren't being watched*; instead, they had sued after discovering *inoperable* video recording equipment whose use had already been discontinued. Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 296-297, 301 (2009).

Fourth, the App Defendants argue that the address book information is not sensitive, so misappropriating it is not highly offensive. However, as argued in the prior round of motions to dismiss, the district court cases cited by the App Defendants are inapposite. They concern automatically-generated computer data sets,[18] web pages visited that have no physical world equivalent,[19] or iterant and impersonal data points.[20] The iDevice address books, by contrast, are human creations that both reveal deeply personal information about their owners—such as the affiliation with and identities of friends, enemies, lovers, ex-lovers, family, doctors, financial institutions, business associates, etc.—and are regularly deemed private.[21] (SCAC ¶¶ 55-60.) The Supreme Court has long held lists of contacts that reveal persons' affiliations to implicate privacy concerns are entitled to heightened protections. NAACP v. Alabama, 357 U.S. 449, 466 (1958) (prohibiting compelled disclosure of membership lists).[22]

---

[18] E.g., In re iPhone Application Litig., 844 F. Supp. 2d at 1050 (automatically generated iDevice identifier number, geolocation information, and in essence the user's gender, age, zip code, and time zone); In re Google Android Consumer Privacy Litig., 2013 WL 1283236 at *2 (collection of personally identifiable information ("PII") and universally unique device identifiers ("UUID")); Yunker, 2013 WL 1282980 at *1.

[19] In re iPhone Application Lit., 844 F. Supp. 2d at 1050, In re Google Inc. Privacy Policy Litig., 2014 WL 3707508 at *2 (aggregation of data generated from using various websites offered and controlled by Google; see In re Google Inc. Privacy Policy Litig., 2013 WL 6248499 for description of data).

[20] E.g., a device's unique identifier (Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1017 (N.D. Cal. 2012)).

[21] See, e.g., United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ("[C]ell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers. Zavala had a reasonable expectation of privacy regarding this information."); see also Riley v. Cal., 134 S. Ct. 2473, 2494-95 (2014) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life[.]'").

[22] Another off-point case the App Defendants cite, Puerto v. Super. Ct., , concerns *litigation discovery* of telephone numbers and addresses of already-identified potential witnesses, not theft of data. 158 Cal. App. 4th 1242, 1248-49 (2008). Plaintiffs' personal contact lists are far more private than a person's mailing address. (Order at 46.) Disturbingly, the App Defendants say that social security numbers are not sensitive data, too – a contention that would probably shock their customers (and flies in the face of the requirement of redacting such information in court-filed documents). The case they cite, Ruiz v. Gap, Inc., 380 F. App'x. 689 (9th Cir. 2010), does not so hold as it merely involved the increased risk of a future disclosure or intrusion into that data, rather than, as alleged here, an actual invasion. Id. at 692-93. Moreover, in Ruiz, the laptop containing the data at issue was *accidentally lost*; not intentionally misappropriated. Id.; see also Belluomini v. Citigroup Inc., No. 3:13–cv–01743, 2013 WL 5645168, *3 (N.D. Cal. Oct. 16,

The App Defendants again attempt to invent a new heightened pleading standard by arguing that Plaintiffs must allege what specific confidential and sensitive information was taken. In the lone case they rely on, In re Yahoo Mail Litig., 2014 WL 3962824, Judge Koh found that as a general matter not all email is private. Id. at *16. Thus, to allege an intrusion of privacy, plaintiffs had to specifically allege what was sensitive about the emails that Yahoo scanned for marketing purposes. Id. at *15. In contrast, here, the entire address book is highly private and sensitive. (SCAC ¶¶ 55-60.)

In sum, as this Court has already found, Plaintiffs have adequately alleged that the App Defendants' invasion of Plaintiffs' privacy was highly offensive. It is up to the jury to decide whether the allegation is true.

2. Plaintiffs Had An Objectively Reasonable Expectation Of Privacy

The App Defendants also argue that Plaintiffs had no reasonable expectation of privacy in their iDevice address books. Their primary "expectation" argument is their insistence that they obtained consent. As discussed above, the alleged facts show otherwise. See Hill, 7 Cal. 4th at 37 ("presence or absence of opportunities to *consent voluntarily* to activities impacting privacy interests obviously affects the expectations of the [plaintiff].") (emphasis added); Hernandez, 47 Cal. 4th at 293-94 (as cited by Instagram, the court found that plaintiffs' lack of consent demonstrated that they had a reasonable expectation of privacy but rejected their privacy claim on other grounds).

Defendants also double down on their "everybody does it" defense, arguing that Plaintiffs could not have a reasonable expectation of privacy because social networking apps work by gathering users' data.[23] Tellingly, they point to no other companies beyond themselves that do

---

2013) (cited as standing for proposition that collection and dissemination of data points are not highly offensive, but decision is not clear as how address and identity data was collected and disclosed by a Ponzi scheme artist).

[23] Kik is an especially big proponent of this theory, arguing that Plaintiffs cannot have an objectively reasonable expectation of privacy because Kik was publicly caught stealing customer data. Kik attempts to rely on Hill and Google Privacy Policy I, where the defendants themselves clearly disclosed their misconduct. Kik cites no case for the proposition that, as a matter of law, a company can continue misappropriating customer information without any liability once its initial misconduct is publicly revealed.

so without prior consent. The mere existence of some members of an industry with a practice of invading consumers' privacy cannot mean that consumers thereby lose their right of privacy. This is especially true here, where this Court found that Plaintiffs have a reasonable expectation of privacy in their iDevice address books (Order at 44-45)–a finding perfectly consistent with subsequent Supreme Court direction in the matter. Riley, 134 S. Ct. at 2494-95.

3. Consent To On-Device Access To Data Is Not Consent To Copy, Upload, And Use The Data

The App Defendants also try to blur the line between a business and its product to argue that, so long as the App had some sort of permission to conduct an on-device look into the user's address book data to "find friends," the App Defendant did not "intrude" on the address book (and thus no privacy violation occurred) by transferring and storing Plaintiffs' address book data at corporate headquarters, despite not having permission to take or upload the data. Whether particular data happens to be private or not (here, it is), permitting your computer or mobile device to crunch data via an on-device software program does not equate to granting the software's maker consent to take a copy of the data for its own use. If it did, Microsoft would be allowed to take copies of every Word document or Excel spreadsheet.

Defendants' all-or-nothing view of privacy also is not the law. Persons can have nuanced expectations of privacy such that one type of access is allowed and one is not. "[P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law." Sanders v. American Broadcasting Companies, Inc., 20 Cal. 4th 907, 916 (1999) (workers had a reasonable expectation of privacy against secret videotaping despite the fact their interactions and conversations were in view of other workers).[24]

[24] Here too the App Defendants rely on cases that are inapposite. Defendants rely on Marich v. MGM/UA Telecomms, 113 Cal. App. 4th 415 (2003), for the proposition that once access is given, there is no intrusion claim for subsequent actions. In that case, plaintiffs sued for invasion of privacy when a television producer recorded their conversation with a police officer, which was then broadcast on a television show. Id. at 419-420. The court upheld the invasion of privacy claim on these facts. It declined to recognize a separate claim for the actions taken at the sound studio to enhance the audio recording for television. Id. at 432. This does not conflict

Accessing a Plaintiffs' address book within their iDevices is entirely different from uploading Plaintiffs' private data to others. The App Defendants cite no authority for their insistence that a permission to look is consent to take.

4. Plaintiffs' Intrusion Damages Need Not Be Specifically Alleged

Finally, the App Defendants argue that Plaintiffs failed to plead damages because the SCAC does not describe the emotional distress they each suffered as a result of the invasion of their privacy. However, as this Court explained, Plaintiffs' existing general damage allegations are sufficient to support a claim for invasion of privacy. (Order at 46.) Damages flowing from an invasion of privacy "logically would include an award for mental suffering and anguish." Miller, 187 Cal. App. 3d at 1484; see also Judicial Council Of California Civil Jury Instruction 1800. Here, Plaintiffs allege that they suffered harm and damages as a result of the App Defendants' invasion of their privacy. (SCAC ¶ 248.) These general damage allegations are sufficient to support Plaintiffs' claim.

5. Plaintiffs' Invasion Of Privacy Claim Establishes Article III Standing

Ignoring the Court's prior order, the App Defendants again argue that Plaintiffs' privacy claim does not satisfy Article III standing. They are still wrong. The standing inquiry exists to determine whether Plaintiffs have a personal stake in the outcome of the controversy. (Order at 40 (citing Baker v. Carr, 369 U.S. 186, 204 (1962).) These indisputably do: it was their mobile devices and their private address books that were intruded upon. As the Court made clear in the last round of pleading, Plaintiffs' allegations are "sufficient to confer standing for those claims on which the injury bears — intrusion upon seclusion[.]" (Order at 41.)

The App Defendants' efforts to tell the Court that it was wrong are baseless. The Ninth Circuit's analysis of Article III standing in Ruiz shows that this Court got it right. The Article III

---

with Plaintiffs' claim, where Plaintiffs allege that App Defendants copied and misused their iDevice address book information. In Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., 306 F.3d 806, 816-18 (2002), the court applied Arizona law to analyze plaintiff's privacy claim based on undercover reporter videotaping conversation without consent, noting that California law is more protective of people's privacy. In Cobbs v. Grant, 8 Cal. 3d 229, 239-41 (1972), the court considered an informed consent claim, where plaintiff gave consent to initial procedure, but not to a necessary additional medical intervention that arose during surgery.

standing inquiry does not require a diminished value analysis, but rather, for an intentional tort such as invasion of privacy, the plaintiff will have standing so long as there is an '"irreducible constitutional minimum' of an injury-in-fact." Ruiz, 380 F. App'x. at 690-91.[25] As discussed above, Plaintiffs' general damage allegations are also sufficient to satisfy both damages and Article III standing. (SCAC ¶ 248; Order at 46.)

Similarly, the App Defendants' reliance on non-analogous cases involving automatically generated "PII" data claims, where plaintiffs alleged economic injury, do not show that "something more is required" here.[26] To the contrary, where plaintiffs have alleged a common law invasion of privacy claim, **nothing more is required** to establish standing.[27] In re Google Android Consumer Privacy Litig., 2013 WL 1283236 at *6-7.

C. CONVERSION

The Court's previous Order granted Plaintiffs leave to amend their pleadings. The SCAC repleads Plaintiffs' conversion claim, emphasizing Plaintiffs' fundamental right to exclude others

---

[25] Similarly, in Citizens for Health v. Leavitt, 428 F.3d 167 (3d Cir. 2005), the court found that plaintiffs demonstrated that at least one of them would have their health information disclosed. Id. at 176, n.9. Here, the SCAC alleges that all of the Plaintiffs had their privacy invaded when the App Defendants intruded upon, accessed, copied, and uploaded their private address books from their iDevices. Thus, the SCAC exceeds the standard set by Citizens for Health.

[26] The four cases Defendants cite were resolved on 12(b)(6) rather than standing grounds. In re Google Inc. Privacy Policy Litig., 2013 WL 6248499 at *4-5 (court did not consider, and it was not alleged, that plaintiffs had standing through a common law privacy claim); In re Google, Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 449-50 (D. Del. 2013) (plaintiffs failed to state a California common law privacy claim); LaCourt v. Specific Media, Inc., No. 10-cv-1256-GW(JCGx), 2011 WL 1661532, *3-4 (C.D. Cal. Apr. 28, 2011) (did not allege a California common law invasion of privacy claim); In re DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (did not allege a California common law invasion of privacy claim).

[27] The App Defendants' assertion that the privacy injury has no constitutional aspect ignores California law. Plaintiffs' invasion of privacy claim necessarily implicates rights provided by Article 1, Section 1 of the California Constitution. Am. Acad. Of Pediatrics v. Lungren, 16 Cal. 4th 307, 326 (1997); Doe v. City & Cnty. of San Francisco, 835 F. Supp. 2d 762, 768 (N.D. Cal. 2011) (the "California Constitution creates a right of action against private parties…[for] two recognized types of privacy interests[.]"). In Yunker, the court found standing on the basis of a constitutional violation. 2013 WL 1282980 at *6; see also Folgelstrom, 195 Cal. App. 4th at 990 (general explanation regarding invasion of privacy claims as constitutional claims).

from possession, obtaining or exercising dominion or control of their property even if, as with many types of intangible property, Defendants' taking and acquisition of the property did not deprive Plaintiffs of their *separate and additional* right to also use the property. (SCAC ¶¶ 90-91, 261, 262.)

The App Defendants move to dismiss this claim for both lack of standing and on the merits, but their (and Apple's related) intertwined arguments amount to the same contention: Defendants insist that no claim for conversion exists unless the property owner is deprived of the use of the property, and that Plaintiffs fail to show any harm under that standard. The former misstates the common law, and the latter fails as a result.

1. California Law Recognizes Claims For Conversion Of Intangible Property Even If The Owner Of The Intangible Property Is Not Deprived Of Use Of It

The App Defendants continue to contend that property like an address book cannot be converted because, even if a copy of the data is wrongfully taken for the defendants' own use, the owner of the data can still use the original data. Though the Court accepted this standing argument on the last briefing round (Order at 40), Plaintiffs respectfully submit that the Court's prior analysis rests on the App Defendants' over-simplification of the law of conversion and disregard of California Civil Code section 3336.

While conversion claims usually involve tangible property[28] (where it is literally not possible for the wrongdoer to take the property without depriving the owner of the ability to use it) deprivation of use is not a *sine qua non* for a conversion claim. An early California Supreme Court case states the common law question is whether the defendant "exercise[s] a dominion over [the property] in exclusion **or in defiance** of the plaintiff's right? If he does, that is in law a conversion." Horton v. Jack, 126 Cal. 521, 526 (1899) (emphasis added). The potential for conversion in defiance of the plaintiff's right, but *not* in exclusion, makes sense because a

[28] California law recognizes the conversion of intangible property. Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003); see also Fremont Indemnity Co. v. Fremont Gen. Corp., 148 Cal. App. 4th 97, 119-126 (2007) (conversion lies for use of net operating loss); Davis v. Electronic Arts Inc., No. 10-03328 RS, 2012 WL 3860819, *9 (N.D. Cal. Mar. 29, 2012) (noting that California Supreme Court has rejected the tangibility requirement).

"fundamental [] [] concept of ownership of personal property is the right to exclude others." eBay, Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058, 1066-67 (N.D. Cal. 2000) (citing Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (characterizing "the right to exclude others" as "one of the most essential sticks in the bundle of rights that are commonly characterized as property")).

Since the time of English common law, courts have recognized that "[o]ne of the main rights attaching to property is the right to exclude others[.]" Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (citing W. Blackstone, *Commentaries*, Book 2, ch. 1) (noting that the same rule applies for both real and personal property); Panduit Corp. v. Stahlin Bros. Fibre Works, Inc., 575 F.2d 1152, 1158 n.5 (6th Cir. 1978) (personal property) ("[t]he right to exclude others is the essence of the human right called 'property.'"); Bell & Parchomovsky, A Theory of Property, 90 Cornell L. Rev. 531, 597 (2005) ("The right to exclude others from using . . . one's property is generally seen as one of the most important rights in property."). "The primary justification for the preeminence of the right to exclude is that it indirectly confers upon the property holder the right to determine the price for using the property and to 'hold out' for greater compensation where others seek entry." Bell & Parchomovsky, 90 Cornell L. Rev. at 598. Though less common than conversion claims involving a physical deprivation, both the Ninth Circuit and California courts recognize conversion claims arising from the appropriation or copying of property because of the violation of this fundamental right to exclude (or to set the price for use). In G.S. Rasmussen Assoc. Inc. v. Kalitta Flying Service, Inc., 958 F.2d 896 (9th Cir. 1992), the defendant refused to pay for the right to use the plaintiff's Supplemental Type Certificate (STC), a type of FAA license for a plane design, but then used it anyway by making a photocopy and using the copy and the STC number on a separate license application. Id. at 899-900. Rasmussen sued for conversion of his STC. Id. Recognizing that "the law generally favors the establishment of property rights," the Ninth Circuit held Rasmussen had a property right in the STC that included the right to exclusive control over it. Id. at 900-03. The court then found that defendant's conduct constituted conversion:

> In California, conversion has three elements: ownership or right to possession of property, wrongful disposition of the property right and damages. …. Our earlier discussion establishes the first element: Rasmussen has an ownership interest in the use of his STC, which is property under California law. **The second requirement is also satisfied: Kalitta photocopied the certificate, presented it to the FAA, and thereby obtained a valuable benefit as a consequence of using Rasmussen's STC without authorization or permission.** Rasmussen has also suffered damages by being denied a return on his investment as a condition for granting Kalitta the right to use his STC. Thus, under California law, Kalitta tortiously converted Rasmussen's STC when it used the STC to obtain airworthiness certification for the modified DC–8.

Id. at 906-07 (emphasis added) (citations omitted).

In reaching this conclusion, the Ninth Circuit cited Lone Ranger Television, Inc. v. Program Radio Corp., 740 F.2d 718, 726 (9th Cir. 1984), where the court affirmed the grant of damages by summary judgment for the plaintiff on a conversion claim where the defendant made and sold unauthorized copies of radio broadcasts of the Lone Ranger. Id. at 726. The Ninth Circuit also cited A&M Records v. Heilman, 75 Cal. App. 3d 554 (1977), where the California Court of Appeal held that making copies of audio recordings (i.e. audio data) and selling them without permission of the original recordings' owner constitutes conversion. Id. at 570 ("misappropriation and sale of the intangible property of another without authority from the owner is conversion."); see also G.S. Gladstone v. Hillel, 203 Cal. App. 3d 977, 989 (1988) (recognizing conversion of copies of jewelry designs).

Just last month, the Central District of California applied this rule in Flo & Eddie Inc. v. Sirius XM Radio Inc., No. CV 13-5693 PSG RZX, 2014 WL 4725382 (C.D. Cal. Sept. 22, 2014). The plaintiff, a corporation formed by the founding members of the band "The Turtles," sued Sirius XM for unauthorized public performances of the plaintiffs' recorded music. The court granted summary judgment in favor of *the plaintiffs* on their conversion claim (and other claims), finding that the defendant committed conversion by using plaintiffs' property without permission. Id. at *11.

Similarly, Judge Koh recently upheld a conversion claim when a defendant failed to buy a distribution license to show a closed-circuit broadcast of a professional boxing match at his

establishment but obtained the data feed and did so anyway. J & J Sports Productions, Inc. v. Ceballos, No. 11-cv-5438-lhk, 2012 WL 4009587 (N.D. Cal. Sept. 12, 2012). The court recognized that such intangible property right was inexhaustible (or infinitely replicable) and that the plaintiff could sell as many iterations of the distribution rights as it desired. Id. at *1. Judge Koh nevertheless explained and determined that plaintiff's allegations of "ownership of the distribution rights to the [p]rogram, misappropriation of those rights by [d]efendant's unlawful interception, and damages" were sufficient to state a conversion claim. Id. at *2 (upholding the claim and awarding damages after entry of a default judgment); see also DIRECTV, Inc. v. Pahnke, 405 F. Supp. 2d 1182, 1189-90 (E.D. Cal. 2005) (conversion of distribution rights for satellite broadcasting); Don King Productions/Kingvision v. Lovato, 911 F. Supp. 419, 423 (N.D. Cal. 1995). Moreover, on virtually identical facts and claims, this Court entered a Default Judgment for the plaintiff that specifically relied on California Civil Code section 3336 to award the plaintiff $2,200 for conversion of the unlicensed broadcast signal and data. J & J Sports Prod., Inc. v. Hernandez, No. 12-cv-05773-JST, 2013 WL 2468354, *3 (N.D. Cal. June 6, 2013).

All of these cases involve valid claims for conversion based on the copying, appropriation, or use of someone's electronic, infinitely-replicable property in violation of the owner's right to control who does so. In none of them was the owner deprived of his or her own ability to use the property. Yet in each case, the Court found a proper claim for conversion. Plaintiffs' lawsuit presents that claim here.

Defendants do not even acknowledge the existence of these cases or the precedent they set. Instead, they rely on non-California law or dicta in cases not squarely presented with this issue. FMC Corp. v. Capital Cities/ABC, Inc., 915 F.2d 300 (7th Cir. 1990), did not address conversion arising from a copy under California law. The court briefly discussed in *dicta* whether copies of tangible documents amounted to conversion under *non-California law*, then noted "[b]ut this case is different." Id. at 303-04 (discussion cited cases that did not analyze California law); see Harper & Row Publishers, Inc. v. Nation Enterprises, 723 F.2d 195, 201 (2d Cir. 1983) (analyzing conversion under other state law and reversed on other grounds by the U.S. Supreme Court, 471 U.S. 539 (1985)); Pearson v. Dodd, 410 F.2d 701, 707 (D.C. Cir. 1969)

(cited by Harper, did not apply California law). FMC Corp.'s dicta does not compel the Court to disregard the clear teaching of G.S. Rasmussen Assoc. Inc., Lone Ranger Television, Inc., and the other cases cited above.[29]

Defendants also argue that an address book is akin to the type of automatically generated "PII" that has been held not subject to conversion.[30] But, as alleged in the SCAC, Plaintiffs' iDevice address books are **not** automatically computer generated information. Plaintiffs input the information in their iDevice address books. (SCAC ¶ 55.) Defendants rely on inapposite cases here. As this Court recognized (Order at 40), Plaintiffs have sufficiently defined their interest in their iDevice address books.

Defendants thus provide no basis for this Court to conclude that Plaintiffs' address books are not property subject to conversion. The fact that Defendants' misappropriation of the address books did not deprive Plaintiffs of the right to use them no more excuses Defendants from the tort of conversion than the same facts did in G.S. Rasmussen Assoc. Inc., Lone Ranger Television, Inc., A&M Records, G.S. Gladstone, J & J Sports Productions, Inc., DIRECTV, Inc., or Don King Productions/Kingvision.

2. Plaintiffs' Alleged Harm From Conversion Satisfies Damages And Article III Standing

The gravamen of the standing inquiry, as this Court has previously noted, is to ascertain whether Plaintiffs are entitled to adjudication of the asserted claim. (Order at 40-41 ("The essence of the standing inquiry is to determine whether the plaintiff has 'alleged such a personal stake in the outcome of the controversy[.]'")); DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 352 (2006). A plaintiff is presumed to be injured when conversion is committed. Cal. Civ. Code

---

[29] Nor does Kremen v. Cohen, require a different result. The Court's analysis in Kremen was focused on whether an intangible domain name could be converted. 337 F.3d at 1030-36. The question of copying was not present in that case.

[30] Defendants cite Yunker, 2013 WL 1282980 at *1 (collection of automatically generated personally identifiable information ("PII") and universally unique device identifiers ("UUID") from use of music app); Low, 900 F. Supp. 2d at 1017 (an automatically generated unique identifier when users visit website); In re iPhone Application Litig., 844 F. Supp. 2d at 1050 (automatically generated iDevice identifier number, geolocation information, and in essence the user's gender, age, zip code, and time zone).

§ 3336 ("detriment caused by the wrongful conversion of personal property is presumed…."). As such, at least nominal damages are always available under California law. Cal. Civ. Code § 3360; see, e.g., Kramer v. Boynton, 258 Cal. App. 2d 171, 175, n. 7 (1968) (in tort claim, court finds that plaintiff at least entitled to nominal damages). That alone satisfies the standing inquiry. See, e.g., Brannian v. City of San Diego, 364 F. Supp. 2d 1187, 1193 (S.D. Cal. 2005); Cramer v. Skinner, 931 F.2d 1020, 1027 (5th Cir. 1991) ("The Constitution draws no distinction between injuries that are large, and those that are comparatively small." "[An] 'identifiable trifle' is sufficient injury to establish standing; standing is not 'to be denied simply because many people suffer the same injury.'" (quoting U.S. v. Students Challenging Regulatory Agency Procedures SCRAP, 412 U.S. 669, 686-87, 689 n. 14 (1973))).

Moreover, the law provides other remedies for a conversion claim. Damages may include "fair compensation for the time and money properly expended in pursuit of the property." Cal. Civ. Code § 3336; Gladstone, 203 Cal. App. 3d at 991 (court awarded compensation to plaintiff for time spent recovering jewelry designs, including copies of designs).

Plaintiffs are also entitled to imposition of a constructive trust "to prevent unjust enrichment and to prevent a person from taking advantage of his or her own wrongdoing." American Master Lease LLC v. Idanta Partners, LTD, 225 Cal. App. 4th 1451, 1484 (2014); Burlesci v. Peterson, 68 Cal. App. 4th 1062, 1069 (1998) (constructive trust is proper remedy for conversion claim). That remedy applies even if the plaintiffs themselves lost no money. "[T]here can be restitution of wrongful gain in cases where the plaintiff has suffered an interference with protected interests but no measurable loss whatsoever." Merrimon v. Unum Life Ins. Co. of America, 758 F.3d 46, 53 (1st Cir. 2014) (quoting Restatement (Third) of Restitution and Unjust Enrichment § 3 reporter's note a (2011)). "[N]o man may take advantage of his own wrong. Deeply rooted in our jurisprudence, this principle has been applied in many diverse classes of cases by both law and equity courts. . . " Glus v. Brooklyn E. Dist. Terminal, 359 U.S. 231, 232-33 (1959); see also Root v. Lake Shore & M.S. Ry. Co., 105 U.S. 189, 207 (1881) (equity requires a wrongdoer to refund illegal profits, "as it would be inequitable that he should make a profit out of his own wrong"); Restatement (Third) of Restitution and Unjust

Enrichment § 3 (2011) ("A person is not permitted to profit by his wrong."). As explained in the recent Restatement of Restitution, this principle "marks one of the cornerstones of the law of restitution and unjust enrichment." Id. at cmt. a. "Salient examples include cases in which a property owner may have suffered no quantifiable injury from the defendant's unlawful interference. Restitution in such cases protects the owner's right to insist that any use of property by another – **whether or not it diminishes the property's value** – be made with the owner's consent and on the owner's terms." Id. at cmt. b (emphasis added). Thus, "it is clear not only that there can be restitution of wrongful gain exceeding the plaintiff's loss, but that there can be restitution of wrongful gain in cases where the plaintiff has suffered an interference with protected interests but **no measurable loss whatsoever**." Id. at note a (emphasis added).

As alleged in the SCAC, Plaintiffs' address books, the product of Plaintiffs' efforts, have both intrinsic and commercial value. (SCAC ¶¶ 54-60.) Defendants benefited from wrongfully taking them.[31] It follows that Plaintiffs have standing to seek redress for this wrong. As such, Plaintiffs' prayer for relief includes a request to impose a constructive trust and prevent Defendants' unjust enrichment. Accordingly, Plaintiffs also have Article III standing to pursue their claim.

D. PLAINTIFFS' CLAIMS ARE NOT PREEMPTED BY THE COPYRIGHT ACT

Several App Defendants insist that the federal Copyright Act preempts Plaintiffs' claims because they involve Defendants' Apps copying Plaintiffs private address book data. In the Ninth Circuit, Copyright Act preemption is a two-step test: (1) the copied materials must be copyrightable subject matter under the Copyright Act; *and* (2) the plaintiff's state law claim must provide rights equivalent to those protected by the Copyright Act. Kodadek v. MTV Networks, Inc., 152 F.3d 1209, 1212 (9th Cir. 1998). The burden is on the defendant to establish both the subject matter prong and the equivalency prong. Here, neither prong is satisfied; therefore, copyright preemption cannot apply.

---

[31] (SCAC ¶¶ 90, 97, 103, 109, 113, 117, 121, 125, 129, 133, 137, 263-270.)

1. Plaintiffs' iDevice Address Books Are Non-Copyrightable Subject Matter Under the Copyright Act

The App Defendants agree that Plaintiffs' address books are *not* subject to copyright protection. (E.g., ECF No. 495 at 9, 11.) This is because lists and databases such as the address book information displayed in a Yellow Pages phone book are not copyrightable subject matter. Feist Publications, Inc. v. Rural Telephone Service Co., Inc., 499 U.S. 340, 344-45 (1991). Nonetheless, the App Defendants contend that Plaintiffs' address books are within the scope of the Copyright Act and, as such, are subject to preemption.

The Copyright Act protects "original works of authorship fixed in any tangible medium of expression." 17 U.S.C. § 102. It expressly excludes ideas. Id. The supposedly "broader" scope of preemption raised in Defendants' motions turns on whether an "idea"—as that term is interpreted under the Act—is sufficiently embodied within a tangible work to fall within copyright preemption, but not protection. Defendants' authority thus relates to a specific and narrow question: Whether an idea not itself in copyrightable form is close enough that Copyright Act preemption applies to a claim for copying that idea. Defendants' cases involve screenplays (Selby v. New Line Cinema Corp., 96 F. Supp. 2d 1053 (C.D. Cal. 2000)), television show ideas (Endemol Entm't B.V. v. Twentieth Television Inc., 48 U.S.P.Q.2d 1524 (C.D. Cal. 1998), Entous v. Viacom Int'l Inc., 151 F. Supp. 2d 1150 (C.D. Cal. 2001)), software designs (Firoozye v. Earthlink Network, 153 F. Supp. 2d 1115 (N.D. Cal. 2001)), and drawings (Kodadek v. MTV Networks, Inc., 152 F.3d 1209 (9th Cir. 1998), Design Art v. Nat'l Football League Props, Inc., No. 00CV593 JM (JAH), 2000 WL 33151646 (S.D. Cal. Aug. 18, 2000)).

Like the non-copyrightable phone listings at issue in Feist, the iDevice address books are not *ideas*. While the facts therein happen to be useful to determine relationships between and how to reach particular people, unexpressive factual information (including unexpressive raw data such as a list of email addresses) like these address books nonetheless fall outside of the realm of copyright protection altogether. See Worth v. Selchow & Righter Co., 827 F.2d 569, 573 (9th Cir. 1987) (copying of trivia book facts for trivial pursuit game not preempted by copyright act); Feist Publications, Inc., 499 U.S. at 344-45. Further, Plaintiffs' iDevice address

books and the address book data are valuable not because they are art or original works of authorship, but because the time and effort Plaintiffs invested and would need to reinvest to gather that same information from everyone they know if they could even find them (or even just to retype that information into their iDevices) is significant.[32] (SCAC ¶¶ 55, 58, 60.) Plaintiffs' iDevice address books thus form useful tools and resources for getting in touch with all of those people, and have substantial commercial value to the App Defendants who harvested them because of the relationships and connections that information reveals. (SCAC ¶¶ 59-60.)

Defendants' reliance on Firoozye is misplaced. Firoozye does not broadly hold that a collection of uncopyrightable facts falls within the scope of Copyright Act preemption. Firoozye, 153 F. Sup. 2d 1115. In Firoozye, the court's analysis turned on the intermingling of non-copyrightable facts with copyrightable software. Id. at 1124-25; see also Meridian Project Systems, Inc. v. Hardin Const. Co., LLC, No. S-04-2728 FCD DAD, 2006 WL 1062070, *4 (E.D. Cal. April 21, 2006) (explaining that an intermingling of software with non-copyrightable facts falls within the scope of the act and are subject to preemption). Plaintiffs do not purport to have created software that was intermingled with their address book data, or that any software was taken by Defendants.

Address books or similar factual materials are simply not sufficiently within the scope of the Copyright Act to trigger preemption. See Dun & Bradstreet Software Services, Inc. v. Grace Consulting, Inc., 307 F.3d 197, 219 (3d Cir. 2002) ("the District Court failed to consider evidence that Geac's customer lists were not copyrightable material and, therefore, that claims alleging a violation of state laws were not preempted."). Because the iDevice address books—the largest set of address book data that an App Defendant could possibly copy from an

---

[32] In Feist Publications, Inc., the Court rejected the Ninth Circuit's "sweat of the brow" theory for copyright protection of compilations of facts. 499 U.S. at 359-61; see also Black's Guide, Inc. v. Mediamerica, Inc., C-90-0819 MHP, 1990 WL 169141, *4 (N.D. Cal. Aug. 15, 1990) (in finding that a regional office leasing guide that presents lists of office space for rent is not protected by the Act, the court explains that the Ninth Circuit no longer recognizes a skill and labor theory for copyright protection of facts).

iDevice—necessarily fall outside the scope of the Copyright Act, claims arising from their misappropriation are not preempted by that Act.

2. Plaintiffs' Conversion and Intrusion Claims Do Not Provide Rights Equivalent To Those Protected By Copyright

Plaintiffs' claims do not confer rights equivalent to those protected by the Copyright Act. For this reason they too are not preempted. In determining whether a state law claim satisfies this second element the court must analyze whether the "violation of the state right is predicated upon an act incorporating elements beyond mere reproduction or the like[.]" G.S. Rasmussen & Associates, Inc. 958 F.2d at 904 (citation omitted). If this is the case, then "there is no preemption." Id.

Defendants' primary attack on the conversion claim rests on the misplaced contention that the SCAC withdrew or abandoned assertions that the App Defendants misused the data. As discussed above, the SCAC does no such thing.[33]

Defendants also argue that conversion claims involving copying are always preempted, relying on Firoozye and Design Art. But those cases do not support their argument. Firoozye instead agrees that "claims for conversion…involve an extra element beyond unauthorized copying since they require a plaintiff to prove that defendant wrongfully obtained possession[]" –precisely what Plaintiffs allege here. Firoozye, 153 F. Supp. 2d at 1130 (citing G.S. Rasmussen & Associates, Inc., 958 F.2d at 904, where the Ninth Circuit declined to apply copyright preemption to a conversion claim of plaintiff's intangible property).

Moreover, the Firoozye plaintiff *voluntarily* "e-mailed a fully operational version" of his *software* to the defendant. Id. at 1118. Similarly, in Design Art, the plaintiff "forwarded to [defendant] [] original drawings of several new proposed designs[.]" 2000 WL 33151646 at *1. Both cases involved the consensual provision of the work at issue to the defendant and dealt with materials in recognized categories of copyrightable subject matter: software (literary works) and

[33] (SCAC ¶¶ 2, 5, 18, 60, 90, 94, 97, 100, 103, 105, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 261, 263.)

drawings (pictorial works). 17 U.S.C § 102(a). Thus, because nothing wrongful preceded the copying itself, these plaintiffs in essence sought damages purely for defendants' unauthorized reproduction of their works. In other words, the copyright claim was coextensive with their conversion claims. Firoozye, 153 F. Supp. 2d at 1130; Design Art, 2000 WL 33151646 at *3.

Here, as discussed above, Plaintiffs did not voluntarily provide Defendants with a copy of their address books. The SCAC alleges that, in addition to obtaining copies of their iDevice address books or portions thereof, App Defendants with Apple's help created Apps that programmatically and improperly accessed the information contained in the address books without permission and misused the obtained information.[34] As a result, Plaintiffs' claim for conversion involves the extra elements of at least (1) a taking without permission, (2) transmitting without permission, and (3) misuse of the stolen address books.

This is not equivalent to the protections afforded by the Act. In accord G.S. Rasmussen & Associates, Inc., 958 F.2d at 904 (no copyright preemption because plaintiff's claim rested on plaintiff's allegation that defendant copied and benefited from the use of the copied information); Lone Ranger Television, Inc., 740 F.2d at 726 (considering duplication of a radio show, the Ninth Circuit found that "the conversion … claim lies outside copyright[.]"); see also Downing v. Abercombie & Fitch, 265 F.3d 994, 1004 (9th Cir. 2001) (misappropriation of likeness not preempted by the act); accord AtPac, Inc. v. Aptitude Solutions, Inc., 787 F. Supp. 2d 1108, 1115 (E.D. Cal. 2011); KNB Enterprises v. Matthews, 78 Cal. App. 4th 362, 372 (2000); see also Chesler/Perlmutter Prods., Inc. v. Fireworks Entm't, Inc., 177 F. Supp. 2d 1050, 1059 (C.D. Cal. 2001) (unjust enrichment claim not preempted by the Act).

The common law right of privacy–to in essence be let alone—is plainly distinct from the rights protected by copyright law. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 199-200 (1890); see also Laws v. Sony Music Entm't, Inc., 448 F.3d 1134, 1145 (9th Cir. 2006) ("To be clear, we recognize that not every right of publicity claim is preempted by the Copyright Act. Our holding does not extinguish common law or

---

[34] (SCAC ¶¶ 90, 94, 100, 105, 111, 115, 119, 123, 127, 131, 135.)

statutory rights of privacy[.]"); see also Downing, 265 F.3d at 1004-05 (invasion of privacy claim not preempted when the act of publication was not key to plaintiff's claim, but rather the use of their likeness).

In sum, Plaintiffs' iDevice address books are not within the scope of the Act. Plaintiffs' claims allege additional elements going beyond the protections provided by the Copyright Act. There is no Copyright Act preemption here.

IV. CONCLUSION

Plaintiffs' complaint against the Defendants provides far more detail than is required under Rule 8 and, if proven, state valid claims against them. The App Defendants' motions should be denied. To the extent, however, that any portion of the App Defendants' motions is granted, Plaintiffs request leave to amend to cure any pleading defect.

Dated: October 10, 2014

By */s/ Michael von Loewenfeldt*
James M. Wagstaffe
Michael J. Von Loewenfeldt
Michael K. Ng
KERR & WAGSTAFFE LLP
101 Mission Street, 18th Floor
San Francisco, CA 94105
Tel: 415-371-8500
Fax: 415-371-0500

By */s/ David M. Given*
David M. Given
Nicholas A. Carlin
PHILLIPS, ERLEWINE & GIVEN LLP
50 California Street, 32nd Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911

Interim Co-Lead Counsel for Plaintiffs

Carl F. Schwenker (TBN 00788374,)
LAW OFFICES OF CARL F. SCHWENKER
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Tel: 512.480.8427
Fax: 512.857.1294

Plaintiffs' Liaison Counsel

Jeff Edwards (TBN 24014406; *pro hac vice*)

EDWARDS LAW
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Telephone: 512.623.7727
Facsimile: 512.623.7729

Jennifer Sarnelli
James S. Notis
Gardy & Notis LLP
560 Sylvan Avenue
Englewood Cliffs, NJ 07632
Tel: (201) 567-7377
Fax: (201) 567-7337

Plaintiffs' Steering Committee ("PSC")

CERTIFICATE OF SERVICE

I hereby certify that on October 10, 2014, I electronically submitted the foregoing OPPOSITION TO APP DEFENDANTS' MOTION TO DISMISS SECOND CONSOLIDATED AMENDED COMPLAINT using the electronic case files system of the court. The electronic case files system sent a "Notice of Electronic Filing" to individuals who have consented in writing to accept this Notice as service of this document by electronic means.

/s/ *Michael von Loewenfeldt*